

JD:JPL
F. #2016R01276

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
-----X

16-785 M

IN THE MATTER OF THE SEARCH
OF INFORMATION ASSOCIATED
WITH TWITTER PROFILE WITH
USERNAME “@naotin58” AT
“http://twitter.com/naotin58” THAT IS
STORED AT PREMISES
CONTROLLED BY TWITTER

FILED UNDER SEAL

APPLICATION FOR A SEARCH
WARRANT FOR INFORMATION IN
POSSESSION OF A PROVIDER
(TWITTER ACCOUNT)

-----X

EASTERN DISTRICT OF NEW YORK, SS:

MEREDITH LEUNG, being duly sworn, hereby deposes and says that she is a
Special Agent with the Department of Homeland Security, Homeland Security Investigations
(“HSI”), duly appointed according to law and acting as such.

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant
for information associated with a certain Twitter account that is stored at premises owned,
maintained, controlled, or operated by Twitter, a social-networking company headquartered
in San Francisco, California. The information to be searched is described in the following
paragraphs and in Attachment A. This affidavit is made in support of an application for a
search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require
Twitter to disclose to the government records and other information in its possession,
pertaining to the subscriber or customer associated with the Twitter account.

2. I have been a Special Agent with HSI (formerly Immigration and Customs Enforcement) and its predecessor agencies for approximately 18 years. I have been assigned to investigate violations of criminal law relating to, among other things, the sexual exploitation of children, immigration crimes, controlled substances and financial frauds.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Upon information and belief, there is probable cause to believe that there is located in INFORMATION ASSOCIATED WITH TWITTER PROFILE WITH USERNAME “@naotin58” AT “http://twitter.com/naotin58” THAT IS STORED AT PREMISES CONTROLLED BY TWITTER (the “SUBJECT ACCOUNT”), further described in Attachment A, the things described in Attachment B, which constitute evidence, fruits and instrumentalities of the possession, access with intent to view, receipt and reproduction of sexually explicit material relating to children, in violation of Title 18, United States Code, Sections 2252 and 2252A.

DEFINITIONS REGARDING CHILD PORNOGRAPHY

5. The following definitions apply to this affidavit and attachments to this affidavit:

- a. “Child Pornography,” as used herein, includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer

image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct), as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct. See 18 U.S.C. §§ 2252 and 2256(2)).

- b. “Visual depictions” include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).
- c. “Sexually explicit conduct” means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. See 18 U.S.C. § 2256(2).
- d. “Internet Protocol address” or “IP address” refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. “Domain name” is a name that identifies an IP address.

PROBABLE CAUSE

6. On or about June 26, 2016, the defendant NAIF ALRASHIDI, the holder and user of the SUBJECT ACCOUNT, arrived at John F. Kennedy International Airport in Queens, New York aboard Qatar Airlines Flight QR 701 from Kuwait City, Kuwait via Doha, Qatar.

7. Upon his arrival, the defendant was selected for an enforcement examination by United States Customs and Border Protection (“CBP”) officers. During the

inspection, the defendant presented one broken iPhone 6S (the “BROKEN PHONE”) and a second iPhone that was powered on (the “WORKING PHONE” and with the BROKEN PHONE, collectively, the “SUBJECT PHONES”).

8. With the consent of the defendant, who unlocked the WORKING PHONE and provided its password, CBP officers performed a manual cursory exam of the WORKING PHONE. During the review of the WORKING PHONE, CBP officers observed multiple images that appeared to be collections of screenshots from different videos. CBP officers observed that a number of the screenshots appeared to involve minors engaged in sexually explicit conduct. For example, one screenshot appeared to depict two boys engaging in anal sex. Another screenshot appeared to depict a young boy about to perform oral sex.

9. The defendant NAIF ALRASHIDI was then advised of his Miranda rights, which he waived. The defendant stated¹ that he had obtained the screenshots on the WORKING PHONE from the Internet; that the BROKEN PHONE contained the same screenshots that were on the WORKING PHONE, as well as an additional approximately three or four videos involving minor males engaged in sexually explicit activity; that he had sent the screenshots to another individual; and that the images on the WORKING PHONE involved boys between the ages of approximately 9 and 10 years old.

10. During his interview with federal agents, the defendant NAIF ALRASHIDI identified the SUBJECT ACCOUNT as his Twitter account. He further stated

¹ Where I refer to statements made by another, including the defendant NAIF ALRASHIDI, I am describing those statements in sum and substance, and in part.

that he conducted one or more searches on Twitter and scrolled through the search results until he found what appeared to be visual depictions of boys and adult men. Thereafter, he “followed” users and groups on Twitter associated with such visual depictions.² Through these searches, the defendant found at least one group that required him to send three videos in order to be able to join the group. ALRASHIDI denied sending any videos.

11. The defendant also stated that he identified additional chat groups on another social-networking application through which it appeared that he could obtain additional videos of boys. Through Twitter, the defendant contacted the administrator of that chat group, asked to the join the group, was granted access and subsequently downloaded approximately seven to eight sexually explicit videos, a portion of which contained visual depictions of young boys.

12. On or about June 27, 2016, the defendant NAIF ALRASHIDI was charged, pursuant to a criminal complaint authorized by the Honorable Steven L. Tiscione, with possession of child pornography, in violation of Title 18, United States Code, Section 2252(a)(4)(B). (See Mag. Docket No. 16-611).

13. Since the date of his arrest the SUBJECT PHONES have been secured by HSI in a forensically sound environment relevant to this investigation. A subsequent forensic examination of the SUBJECT PHONES revealed that the Twitter application was installed on both phones and that the BROKEN PHONE was in use since at least in or about March 2016.

² As described in greater detail below, a Twitter user can “follow” other Twitter users, which means subscribing to those users’ Tweets and site updates. (See ¶ 26).

14. On or about August 2, 2016, the government submitted a letter to Twitter, pursuant to Title 18, United States Code, Section 2703(f), requesting that Twitter to preserve all stored communications, records, and other evidence currently in its possession regarding the SUBJECT ACCOUNT.

**USE OF COMPUTERS AND MOBILE DEVICES
REGARDING CHILD PORNOGRAPHY**

15. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed and utilized. Prior to the advent of computers and the Internet, child pornography was produced using cameras and film, resulting in either still photographs or movies. The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these images on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls, and compensation for these wares would follow the same paths. More recently, through the use of computers and the Internet, distributors of child pornography use websites, e-mail accounts, social-networking tools and computers to conduct business, allowing them to remain relatively anonymous. Computers are used by individuals who exploit children (including collectors of child pornography) to locate, view, download, collect and organize images of child pornography found through the Internet.

16. In addition, the development of computers has also revolutionized the way in which child pornography collectors interact with, and sexually exploit, children. Computers serve four basic functions in connection with child pornography: production, communication, distribution, and storage. More specifically, the development of computers has changed the methods used by child pornography collectors in these ways:

a. Producers of child pornography can now produce both still and moving images directly from a common video camera, digital camera or mobile telephone. The camera is attached, using a device such as a cable, wirelessly or digital images are often uploaded from the camera's memory card, directly to the computer. Additionally, many mobile phones and computing devices have built-in cameras. Images can then be stored, manipulated, transferred, or printed directly from the computer or mobile device. Images can be edited in ways similar to how a photograph may be altered. Images can be lightened, darkened, cropped, or otherwise manipulated. The producers of child pornography can also use a device known as a scanner to transfer photographs into a computer-readable format. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography. In addition, there is an added benefit to the pornographer in that this method of production does not leave as large a trail for law enforcement to follow. Additionally, digital cameras, video gaming systems, mobile telephones and digital cameras themselves may be used as storage and editing devices for images of child pornography, even where such child pornography images were not created using these devices.

b. The Internet and e-mail accounts allow any computer to connect to another computer. By connecting to a host computer, electronic contact can be made to literally millions of computers around the world. These service providers act as a gateway for their subscribers to the Internet or the World Wide Web. The Internet allows users, while still maintaining anonymity, to easily locate other individuals with similar interests in child pornography and websites that offer images of child pornography. Child pornography collectors can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages, which promote anonymity for both the distributor and recipient, are well known and are the foundation of transactions between child pornography collectors over the Internet.

c. The computer's capability to store images in digital form makes it an ideal repository for child pornography. For example, a memory card within a digital device can store dozens of videos and hundreds of images. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers and mobile devices has grown tremendously within the last several years. These items can store thousands of images and video clips at very high resolution. It is possible to use a mobile telephone to capture an image, process that image and save that image to storage in another country without using any other device whatsoever.

TECHNICAL INFORMATION ABOUT TWITTER

17. Twitter owns and operates a free-access social-networking website of the same name that can be accessed at <http://www.twitter.com>. Twitter allows its users to create their own profile pages, which can include a short biography, a photo of themselves, and location information. Twitter also permits users create and read 140-character messages called “Tweets,” and to restrict their “Tweets” to individuals whom they approve. These features are described in more detail below.

18. Upon creating a Twitter account, a Twitter user must create a unique Twitter username and an account password, and the user may also select a different name of 20 characters or fewer to identify his or her Twitter account. The Twitter user may also change this username, password, and name without having to open a new Twitter account.

19. Twitter asks users to provide basic identity and contact information, either during the registration process or thereafter. This information may include the user’s full name, e-mail addresses, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, and other personal identifiers. For each user, Twitter may retain information about the date and time at which the user’s profile was created, the date and time at which the account was created, and the IP address at the time of sign-up. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access a given Twitter account.

20. A Twitter user can post a personal photograph or image (also known as an “avatar”) to his or her profile, and can also change the profile background or theme for his

or her account page. In addition, Twitter users can post “bios” of 160 characters or fewer to their profile pages.

21. Twitter also keeps IP logs for each user. These logs contain information about the user’s logins to Twitter including, for each access, the IP address assigned to the user and the date stamp at the time the user accessed his or her profile.

22. As discussed above, Twitter users can use their Twitter accounts to post “Tweets” of 140 characters or fewer. Each Tweet includes a timestamp that displays when the Tweet was posted to Twitter. Twitter users can also “favorite,” “retweet,” or reply to the Tweets of other users. In addition, when a Tweet includes a Twitter username, often preceded by the “@” sign, Twitter designates that Tweet a “mention” of the identified user. In the “Connect” tab for each account, Twitter provides the user with a list of other users who have “favorited” or “retweeted” the user’s own Tweets, as well as a list of all Tweets that include the user’s username (i.e., a list of all “mentions” and “replies” for that username).

23. Twitter users can include photographs or images in their Tweets. Each Twitter account also is provided a user gallery that includes images that the user has shared on Twitter, including images uploaded by other services.

24. Twitter users can also opt to include location data in their Tweets, which will reveal the users’ locations at the time they post each Tweet. This “Tweet With Location” function is off by default, so Twitter users must opt in to the service. In addition, Twitter users may delete their past location data.

25. When Twitter users want to post a Tweet that includes a link to a website, they can use Twitter's link service, which converts the longer website link into a shortened link that begins with <http://t.co>. This link service measures how many times a link has been clicked.

26. A Twitter user can "follow" other Twitter users, which means subscribing to those users' Tweets and site updates. Each user profile page includes a list of the people who are following that user (i.e., the user's "followers" list) and a list of people whom that user follows (i.e., the user's "following" list). Twitter users can "unfollow" users whom they previously followed, and they can also adjust the privacy settings for their profile so that their Tweets are visible only to the people whom they approve, rather than to the public (which is the default setting). A Twitter user can also group other Twitter users into "lists" that display on the right side of the user's home page on Twitter. Twitter also provides users with a list of "Who to Follow," which includes a few recommendations of Twitter accounts that the user may find interesting, based on the types of accounts that the user is already following and who those people follow.

27. In addition to posting Tweets, a Twitter user can also send Direct Messages ("DMs") to one of his or her followers. These messages are typically visible only to the sender and the recipient, and both the sender and the recipient have the power to delete the message from the inboxes of both users. As of January 2012, Twitter displayed only the last 100 DMs for a particular user, but older DMs are stored on Twitter's database.

28. Twitter users can configure the settings for their Twitter accounts in numerous ways. For example, a Twitter user can configure his or her Twitter account to

send updates to the user's mobile phone, and the user can also set up a "sleep time" during which Twitter updates will not be sent to the user's phone.

29. Twitter includes a search function that enables its users to search all public Tweets for keywords, usernames, or subject, among other things. A Twitter user may save up to 25 past searches.

30. Twitter users can connect their Twitter accounts to third-party websites and applications, which may grant these websites and applications access to the users' public Twitter profiles.

31. If a Twitter user does not want to interact with another user on Twitter, the first user can "block" the second user from following his or her account.

32. In some cases, Twitter users may communicate directly with Twitter about issues relating to their account, such as technical problems or complaints. Social-networking providers like Twitter typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. Twitter may also suspend a particular user for breaching Twitter's terms of service, during which time the Twitter user will be prevented from using Twitter's services.

33. As explained herein, information stored in connection with a Twitter account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. Based on my training and experience, a Twitter user's account information, IP log, stored electronic

communications, and other data retained by Twitter, can indicate who has used or controlled the Twitter account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, profile contact information, communications, “tweets” (status updates) and “tweeted” photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Twitter account at a relevant time. Further, Twitter account activity can show how and when the account was accessed or used. For example, as described herein, Twitter logs the Internet Protocol addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Twitter access, use, and events relating to the crimes under investigation. Additionally, Twitter builds geo-location into some of its services. If enabled by the user, physical location is automatically added to “tweeted” communications. This geographic and timeline information may tend to either inculcate or exculpate the Twitter account owner. Last, Twitter account activity may provide relevant insight into the Twitter account owner’s state of mind as it relates to the offense under investigation. For example, information on the Twitter account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a criminal plan) or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

34. Therefore, the computers of Twitter are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Twitter, such as account access information, transaction information, and other account information.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

35. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Twitter to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

36. Based on the forgoing, I respectfully request that the Court issue the proposed search warrant.

37. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) and (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

38. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

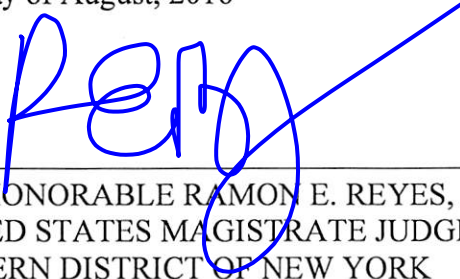
REQUEST FOR SEALING

39. I further respectfully request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.



MEREDITH LEUNG
Special Agent
U.S. Department of Homeland Security,
Homeland Security Investigations

Sworn to before me this
24th day of August, 2016



THE HONORABLE RAMON E. REYES, JR.
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A
Property to Be Searched

This warrant applies to information associated with the Twitter profile with username “@naotin58” at “http://twitter.com/naotin58” that is stored at premises owned, maintained, controlled, or operated by Twitter, a company headquartered in San Francisco, California.

ATTACHMENT B
Particular Things to be Seized

I. Information to be disclosed by Twitter

To the extent that the information described in Attachment A is within the possession, custody, or control of Twitter, including any messages, records, files, logs, or information that have been deleted but are still available to Twitter, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Twitter is required to disclose the following information to the government for each account listed in Attachment A:

- a. All identity and contact information, including full name, e-mail address, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, and other personal identifiers;
- b. All past and current usernames, account passwords, and names associated with the account;
- c. The dates and times at which the account and profile were created, and the Internet Protocol (“IP”) address at the time of sign-up;
- d. All IP logs and other documents showing the IP address, date, and time of each login to the account;
- e. All data and information associated with the profile page, including photographs, “bios,” and profile backgrounds and themes;
- f. All “Tweets” and Direct Messages sent, received, “favorited,” or retweeted by the account, and all photographs, images or videos included in those Tweets and Direct Messages;
- g. All information from the “Connect” tab for the account, including all lists of Twitter users who have favorited or retweeted Tweets posted by the account, as well as a list of all Tweets that include the username associated with the account (i.e., “mentions” or “replies”);
- h. All photographs, images and videos in the user gallery for the account;
- i. All location data associated with the account, including all information collected by the “Tweet With Location” service;
- j. All information about the account’s use of Twitter’s link service, including all longer website links that were shortened by the service, all resulting shortened links, and all information about the number of times that a link posted by the account was clicked;

- k. All data and information that has been deleted by the user;
- l. A list of all of the people that the user follows on Twitter and all people who are following the user (i.e., the user's "following" list and "followers" list);
- m. A list of all users that the account has "unfollowed" or blocked;
- n. All "lists" created by the account;
- o. All information on the "Who to Follow" list for the account;
- p. All privacy and account settings;
- q. All records of Twitter searches performed by the account, including all past searches saved by the account;
- r. All information about connections between the account and third-party websites and applications;
- s. All records pertaining to communications between Twitter and any person regarding the user or the user's Twitter account, including contacts with support services, and all records of actions taken, including suspensions of the account.

II. Information to be Seized by the Government

All information described above in Section I that constitutes evidence, fruits and instrumentalities of the possession, access with intent to view, receipt and reproduction of sexually explicit material relating to children, in violation of Title 18, United States Code, Sections 2252 and 2252A since March 1, 2016, including, for each user ID identified on Attachment A, information pertaining to the following matters:

- a. Images of child pornography and files containing images of child pornography and records, images, information or correspondence pertaining to the possession, access with intent to view, receipt and reproduction of sexually explicit material relating to children, in violation of Title 18, United States Code, Sections 2252 and 2252A, in any form wherever they may be stored or found;
- b. Records, information or correspondence pertaining to the possession, access with intent to view, transportation, receipt, distribution and reproduction of sexually explicit material relating to children, as defined in 18 U.S.C. § 2256;

- c. Records establishing possession, access to, or transmission through interstate or foreign commerce of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;
- d. Records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.
- e. Evidence indicating how and when the Twitter account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Twitter account owner;
- f. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).
- g. The identity of the person(s) who communicated with the user ID about matters relating to the possession, access with intent to view, receipt and reproduction of sexually explicit material relating to children, including records that help reveal their whereabouts.